REMARKS

The examiner rejected claims 1-39 under 35 U.S.C. 102(e) as being anticipated by Yavatkar, et al. (US 6,735,702).

Applicant's claims are allowable over Yavatkar et al. For example, the cited reference neither describes nor suggests a monitoring process that monitors network traffic through the gateway, and a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center, as recited in claim 1.

The examiner contends that:

> **Yavatkar, et al. (US 6,735,702) discloses gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device comprises: a computing device comprising: a monitoring process that monitors network traffic through the gateway; [col. 2, lines 53-55 and col.7, lines 43-44] a communication process that can communicate statistics collected [col. 2, lines 4-5 and col. 10, lines 15-16] in the gateway from the monitoring process with a control center and that can receive queries or instructions from the control center; [col.3, lines 25-29 and col. 11, lines 51-55] and a filtering process to allow filters to be inserted to filter out packets that the gateway deems to be part of an attack. [col. 13, lines 53-62 and col.20, lines 20-21]**

In none of the cited passages of Yavatkar or elsewhere, does Yavatkar, et al.disclose or suggest a communication process that can communicate statistics collected in the gateway from the monitoring process with a control center and that can receive queries or instructions from the control center.

The examiner contends that this feature is taught at [col. 2, lines 4-5 and col. 10, lines 15-16] and [col.3, lines 25-29 and col. 11, lines 51-55]. At those passages Yavatkar discusses::

> **A sniffer is a device which may record network statistics at a node. [col. 2, lines 4-5].**
>
> **Worksheets 234-38 may perform tasks such as monitoring port statistics, CPU utilization, or reachability to other nodes. Worksheets 234-38 may use services to perform some tasks. Code segment 220 includes a controlling method 242, the first method invoked when agent 110 is started on a node, which may contain code controlling agent 110 and executing work object 222. Controlling method 242 controls the overall operation of agent 110; controlling method 110 may invoke other methods of agent 110 or other methods made available by the proactive environment or JVM on which agent 110 operates (not shown). [col. 10, lines 15-16].**

> **The system and method of an exemplary embodiment of the present invention use agents--mobile software modules--to collect data on the state of a network during a network attack, allowing for more accurate diagnosis of an attack. During a network attack, the system and method of the present invention allow for details on the attack traffic (e.g., the source of the attack traffic and path of the attack traffic) to be gathered. The source of the attack traffic may be the originator of the attack traffic or, for example a gateway allowing attack traffic to enter a network and which is, in effect, the source of attack traffic to the network. Such information then may be used to halt the attack or insulate the network from the attack. [col.3, lines 25-29].**
>
> **An agent may manage devices via services which are provided on a proxy device which can be used to monitor or control managed devices via, for example, SNMP or command line interface ("CLI"). Thus an agent may access, for example, data on a port on a remote device. [col. 11, lines 51-55]**

Nowhere in those passages or elsewhere is disclosed this feature of Applicant's claim 1. While Yavatkar discloses a sniffer device, the sniffer device does not suggest the feature of: "a communication process that can communicate statistics collected in the gateway from the monitoring process with a control center and that can receive queries or instructions from the control center," as in claim 1. Rather, Yavatkar discloses in the background (col. 2 lines 27-44) that:

> **Systems exist for collecting information about network traffic. For example, to determine the node which is the source of attack traffic (or the gateway allowing such traffic into a network, which in such a case may be considered a source) and the path or paths taken by such traffic, a human operator may access each link at a node receiving such traffic and analyze the incoming traffic using a sniffer. A sniffer is a device which may record network statistics at a node. The operator may identify which of the physical links attached to the node is receiving a certain type or amount of traffic and then move to the node on the other end of the identified link. The path or paths of traffic from the source of the traffic may be found by traversing the network from node to node, using the sniffer at each node in a path, until the source is reached. Such a diagnosis is slow and inaccurate. A similar analysis may be performed from a central console which may query remote nodes for information about the source of incoming traffic. Such a diagnosis is also slow and inaccurate, as it requires commands to nodes and responses from nodes to be transmitted across the network. The speed at which attacks occur and the speed at which such problems must be fixed makes such detection methods ineffective. A path taken by traffic may be described as the equipment traversed by traffic as the traffic crosses a network or networks (e.g., a series of nodes and links, or a series of sub-networks**

Yavatkar discloses a sniffer as a device which may record network statistics at a node. However, according to Yavatkar an operator identifies which of the physical links attached to the

node is receiving a certain type or amount of traffic and then move to the node on the other end of the identified link.

Yavatkar also discloses the use of agents "mobile software modules" to collect data on the state of a network during a network attack. However, Yavatkar also discloses that an agent may manage devices via services provided on a proxy device to monitor or control managed devices. Yavatkar says nothing that could suggest a communication process that communicate statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center. Yavatkar's disclosed agents do not communicate statistics collected in the gateway or receives queries from a control center. Neither the agent nor the sniffer receives queries from a communication process running on a gateway.

In contrast, Yavatkar specifically teaches away from any use of a control center at Col. 4 lines 24-38.

> **Gathering information about a network attack using mobile agents is much quicker than gathering such information by having a human operator travel from node to node, and is also quicker than polling nodes from a central location. Network attacks may start and stop quickly; the only effective diagnosis may be one that takes place during this brief period. Mobile agents may determine, without exchanging information or commands from a central location or human operator, which path to take to further investigate an attack. Since communication between a central console and a remote node is not required, a finer granularity of information may be collected and acted upon. Accuracy is improved by the speed at which agents may gather, process, and act on information.**

Accordingly, Yavatkar cannot suggest much less describe this feature of claim 1.

Claim 1 also includes the feature of a filtering process to allow filters to be inserted to filter out packets that the gateway deems to be part of an attack. The examiner also contends that this feature is disclosed at [col. 13, lines 53-62 and co1.20, lines 20-21]. Those passages are also reproduced below:

> **source device--the sender of the attack traffic inserts a false "return address."**
>
> **In a network having multiple gateways to other networks, if the particular gateway allowing attack traffic onto the network can be identified, the attack can be halted. Either the gateway can be shut down or the appropriate filter can be**

> **installed on the gateway. However, using current methods to identify the gateway which is, in effect, the source of attack traffic to the network can be difficult and time consuming. A network administrator using a sniffer may determine which physical link (of multiple links) on a device receiving attack traffic is the source of such traffic. Certain modules resident on nodes may perform similar functions under the direction of a central console. With such information a network administrator may move from node to node, tracing the path of the hostile messages from the victim to the source, or to the gateway allowing such traffic to enter the network. Such a method of determining the source of messages is slow.**

Claim 1 requires that the filters be inserted based remove packets that the gateway deems to be part of the attack. Yavatkar however teaches to shut down the gateway or to insert filters. However, in Yavatkar, that decision is performed by an administrator using a sniffer that determines a physical link or certain modules under direction of a central console, not as in claim 1 where a computing device includes a filtering process the filter removes packets that the gateway deems to be part of the attack. Yavatkar also discloses that with such information a network administrator moves from node to node, tracing the path of the hostile messages from the victim to the source or to the gateway allowing such traffic to enter the network. Yavatkar acknowledges that such a method of determining the source of messages is slow. Yavatkar proposes to address this by use of watchdog and bloodhound agents discussed starting at Col. 14, line 18. Therefore, Yavatkar fails to teach to insert filters to filter out packets that the gateway deems to be part of an attack.

Claims 2-15 are also allowable over Yavatkar at least for the reasons given in claim 1.

Claim 2 serves to further distinguish over Yavatkar. In claim 2, the communication process couples to a dedicated link to communicate with the control center over a hardened network. The examiner contends that this feature is disclosed at col. 2, lines 57-59; discussing "the communication process couples to a dedicated link to communicate with the control center over a hardened network." Applicant disagrees. Yavatkar col. 2, lines 57-59 is set forth below:

> **A method and system are disclosed for analyzing traffic on a network by monitoring network traffic and, when a particular network condition (for example, a network attack) is detected, gathering information about the traffic on the network by launching an agent and having the agent iteratively identify which of the links on the node on which the agent operates accepts a type or class of traffic, traverse the identified link to the node across the link, and repeat the process.**

It is clear from that passage that neither there nor elsewhere does Yavatkar disclose or suggest that the communication process communicates with the control center over a hardened network. Rather, as discussed above, Yavatkar in the background teaches away by the disclosure that: "Such a diagnosis is also slow and inaccurate, as it requires commands to nodes and responses from nodes to be transmitted across the network." In addition, as taught by Yavatkar own contribution, communication is performed using the network that is being monitored.

Claim 5 serves to distinguish since Yavatkar does not disclose that the gateway is adaptable to dynamically install filters on nearby routers. Yavatkar teaches in the passage cited by the examiner that the gateway can act as a firewall. A firewall does not suggest to dynamically install filters on nearby routers.

Claim 6 recites that the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets. The examiner cites Yavatkar Col 13, lines 4-29 and Col. 15, lines 30-33. However, this discussion deals with details of a SYN-ACK attack, whereas the teaching at Col. 15 deals with looking for invalid return addresses. Neither passage suggests detecting IP traffic and determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

Claim 7 recites that the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses. The examiner contends: "As per claim 7: See col.13, lines 44-53 and col. 15, lines 19-21; discussing the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses." Applicant contends that no such teachings are found in the cited passages.

Claim 8 recites that the monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports. The examiner contends that: "As per claim 8: See col. 13, lines 4-29 and col. 15, lines 30-33; discussing monitoring process detects Internet Protocol (IP) traffic and

determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports." Applicant contends that no such teachings are found in the cited passages.

Claim 9 recites that the monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection. As per claim 9: See col. 15, lines 30-33; discussing monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection. Applicant contends that no such teachings are found in the cited passages.

Claim 10 recites that the monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection. The examiner contends that: "As per claim 10: See col. 1, lines 27-31; discussing monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection." Applicant contends that no such teachings are found in the cited passages.

Claim 11 recites that the monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail. The examiner contends that: "As per claim 11: See col.2, lines 53-55; discussing monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail." Applicant contends that no such teachings are found in the cited passages.

Claim 12 recites that the monitoring process maintains statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction. The examiner contends that: "As per claim 12: See col.2, lines 4-5 and col.3, lines 30-32; discussing monitoring process maintains statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction." Applicant contends that no such teachings are found in the cited passages. At Col. 2 lines 4-5 Yavatkar discusses that a sniffer device can collect statistics. At Col. 3, lines 30-32 Yavatkar discusses "During a

network attack, the system and method of the present invention allow for details on the attack traffic (e.g., the source of the attack traffic and path of the attack traffic) to be gathered." Later in the same paragraph, Yavatkar further discloses that:

> **The source of the attack traffic may be the originator of the attack traffic or, for example a gateway allowing attack traffic to enter a network and which is, in effect, the source of attack traffic to the network. Such information then may be used to halt the attack or insulate the network from the attack.**

Yavatkar does not suggest to maintain statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction in either of these passages. Moreover, the combination of these passages is not suggested since the first passage regarding the sniffer is in the background and Yavatkar specifically teaches away from that device.

Claim 13 recites that the monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold. The examiner contends: "As per claim 13: See col.14, lines 54-58.and col.15, lines 26-27; discussing monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold. While Yavatkar issues warnings, it is clear that the watchdog nodes referred to by Yavatkar do not disclose the features configurable thresholds determining when a measured parameter exceed the threshold. Yavatkar does not appear to operate using thresholds on collected statistics.

Claims 16 to 39 and their respective dependent claims are allowable over Yavatkar for analogous reasons as those given above for claims 1-15.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

All of the dependent claims are patentable for at least the reasons for which the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made

arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Enclosed is a **$510** check for the Petition for Extension of Time fee. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 1/20/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21180774.doc